IoT 2020

Is Your Home Becoming a Spy? A Data-Centered Analysis and Classification of Smart Connected Home Systems

Presenter: Joseph Bugeja

Authors: Joseph Bugeja, Andreas Jacobsson, Paul Davidsson

MALMÖ UNIVERSITY
INTERNET OF THINGS AND PEOPLE RESEARCH CENTER

KK-stiftelsen

INTRODUCTION

✓ A smart connected home is essentially a residence consisting of Internet of Things (IoT) systems that can be managed over the Internet, typically via mobile apps.

Image: Shutterstock

INTRODUCTION

✓ A smart connected home contains a heterogenous amount of IoT systems.

Connected devices

Apps

iOS

android

Windows Phone

✓ These systems leverage sensors to collect data from users and their environment.

RESEARCH AIMS

Help researchers better understand the privacy implications and what is at stake with different smart connected home systems.

RESEARCH CONTRIBUTIONS

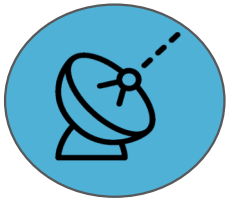
i. Classification of connected home systems based on their data collection capabilities;

ii. A quantitative survey of connected home systems in terms of their data collection capabilities; and

iii. Identifying research directions and best practices to minimize privacy risks of smart connected home systems.

Cameras

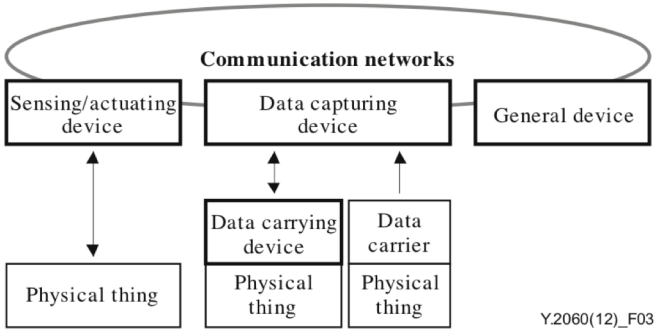
Microphone



Location trackers

SOME RELATED WORK

✓ Device type and functionality, e.g., ITU[1]



1. ITU Telecommunication Standardization Sector. 2012. Recommendation ITU-TY. 2060: Overview of the Internet of things. (2012), 2060–201206.

and other contributions but...

mann et al.[2]

Name	data		
Class 0, C0	<< 1		
Class 1, C1	~ 10 KiB	~ 100 KiB	
Class 2, C2	~ 50 KiB	~ 250 KiB	

Table 1: Classes of Constrained Devices (KiB = 1024 bytes)

2. Carsten Bormann, Mehmet Ersue, and Ari Keranen. 2014. RFC 7228: Terminology for Constrained-Node Networks. IETF Request For Comments (2014).

✓ Functional capabilities, e.g., Kumar et al.[3]

Wearable (e.g., Fitbit, Apple Watch)
Game Console (e.g., XBox)
Home Automation (e.g., Nest Thermostat)
Storage (e.g., home NAS)
Surveillance (e.g., IP camera)
Work Appliance (e.g., printer or scanner)
Home Voice Assistant (e.g., Alexa)
Vehicle (e.g., Tesla)
Media/TV (e.g., Roku)
Home Appliance (e.g., smart fridge)
Generic IoT (e.g., toothbrush)

3. Deepak Kumar et al. 2019. All things considered: an analysis of IoT devices on home networks. In 28th {USENIX} Security Symposium ({USENIX} Security 19). 1169–1185.

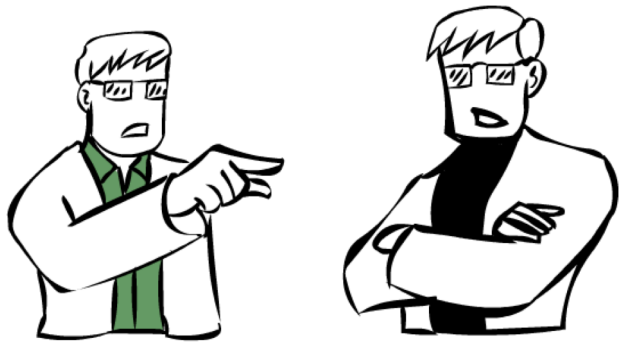
MAIN OBSERVATIONS

i. Tend to be prone to subjectivity and biases;

ii. Difficult to mathematically justify the classification;

iii. Tedious to recreate the classification; and

iv. Shortage of classifications that are derived empirically from the technical specs of commercial systems.



DEVELOPING THE CLASSIFICATION

1

Data Collection

moz://a *privacy not included

- Energy & resource management
- Entertainment
- Health and wellness
- Human-machine interface
- Household appliances and kitchen aids
- Security and safety

2

Data Processing

81 systems

Sensor

{0|1}

Deployment

{0|1}

3

Data Analysis

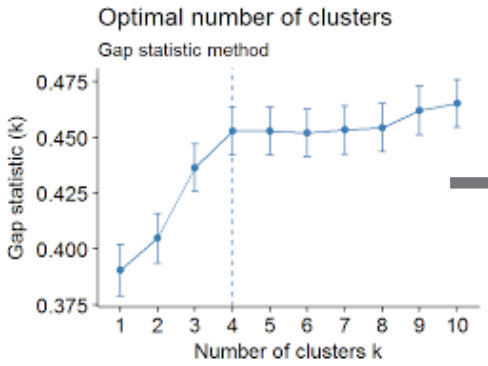
CSV

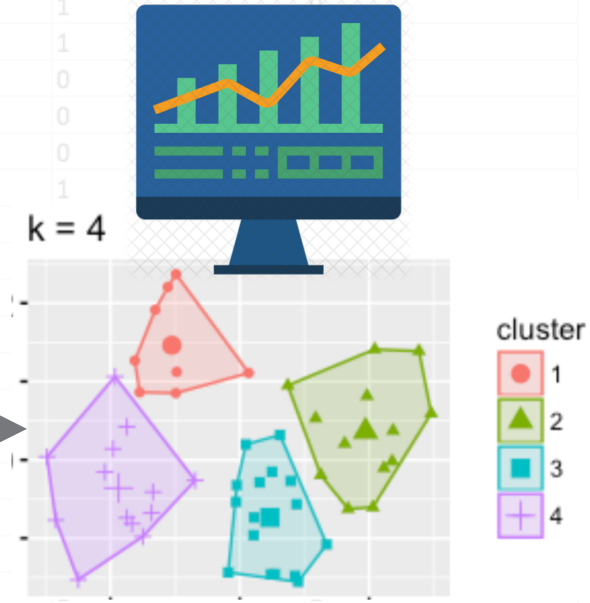
Product,
Sensor {0|1},
Deployment {0|1}.

DEVELOPING THE CLASSIFICATION

Product	Camera Device	Camera App	Microphone Device	Microphone App	Location Device	Location App
Amazon Cloud Cam Security Camera	1	1	1	1	0	1
Amazon Echo & Dot	0	1	1	1	1	1
Amazon Fire HD Kids Edition	1	0	1	0	1	0
Amazon Fire HD Tablet	1	0	1	0	1	0
Amazon Fire TV	0	0	1	1	1	1
Anova Precision Cooker Sous Vide	0	0	0	0	0	1
Apple Airpods	0	1	1	1	0	1
Apple Homepod	0	0	1	0	0	0
Apple iPad	1	0	1	0	1	0
Apple TV	0	0	1	0	1	0
Apple Watch 4	0	0	1	0	0	1
Athena Safety Wearable	0	1	0	0	0	1
Beautyrest Sleeptracker	0	1	0	0	0	1
Beautyrest SmartMotion Base	0	1	0	0	0	1
Beeline Smart Bike Compass	0	0	0	0	0	1
Bose QuietComfort 35 II	0	0	1	1	0	1
CogniToys Dino	0	0	1	0	0	1
Cue the Robot	0	0	1	1	0	0
Dash the Robot	0	0	1	1	1	1
DJI Spark Selfie Drone	0	1	1	1	1	1
Dobby Pocket Drone	0	1	1	1	1	1
Dot Creativity Kit	0	0	1	1	1	1
Eight Sleep Mattress	0	0	0	0	0	1
Findster Duo Plus Pet Tracker	0	1	0	1	1	1

DEVELOPING THE CLASSIFICATION





Systems **R Studio** **Gap statistic** **K-means clustering**

CLASSIFICATION OF SYSTEMS

Listeners

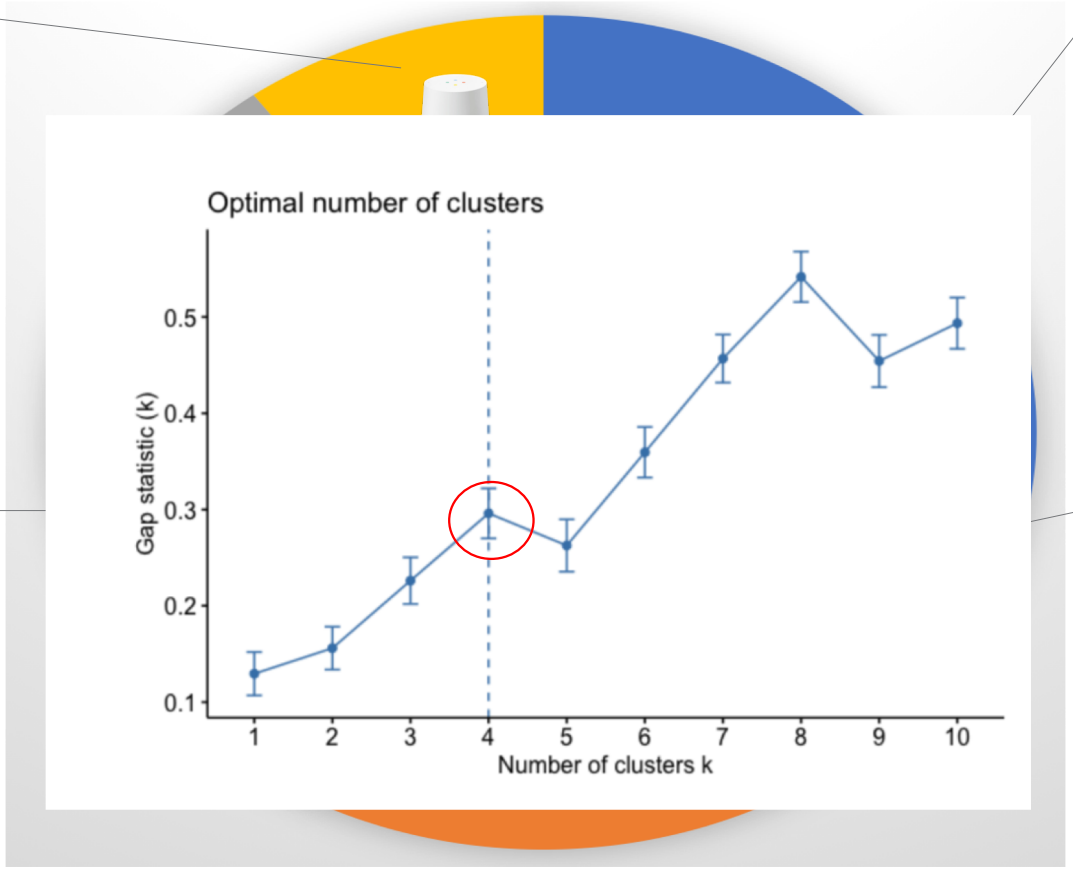
Primarily designed to capture audio data from users.

E.g., Google Home.

App-based accessors

Predominately utilize mobile apps to collect data from users.

E.g., Amazon Fire TV Stick.



Location harvesters

Focused on capturing precisely the location of users.

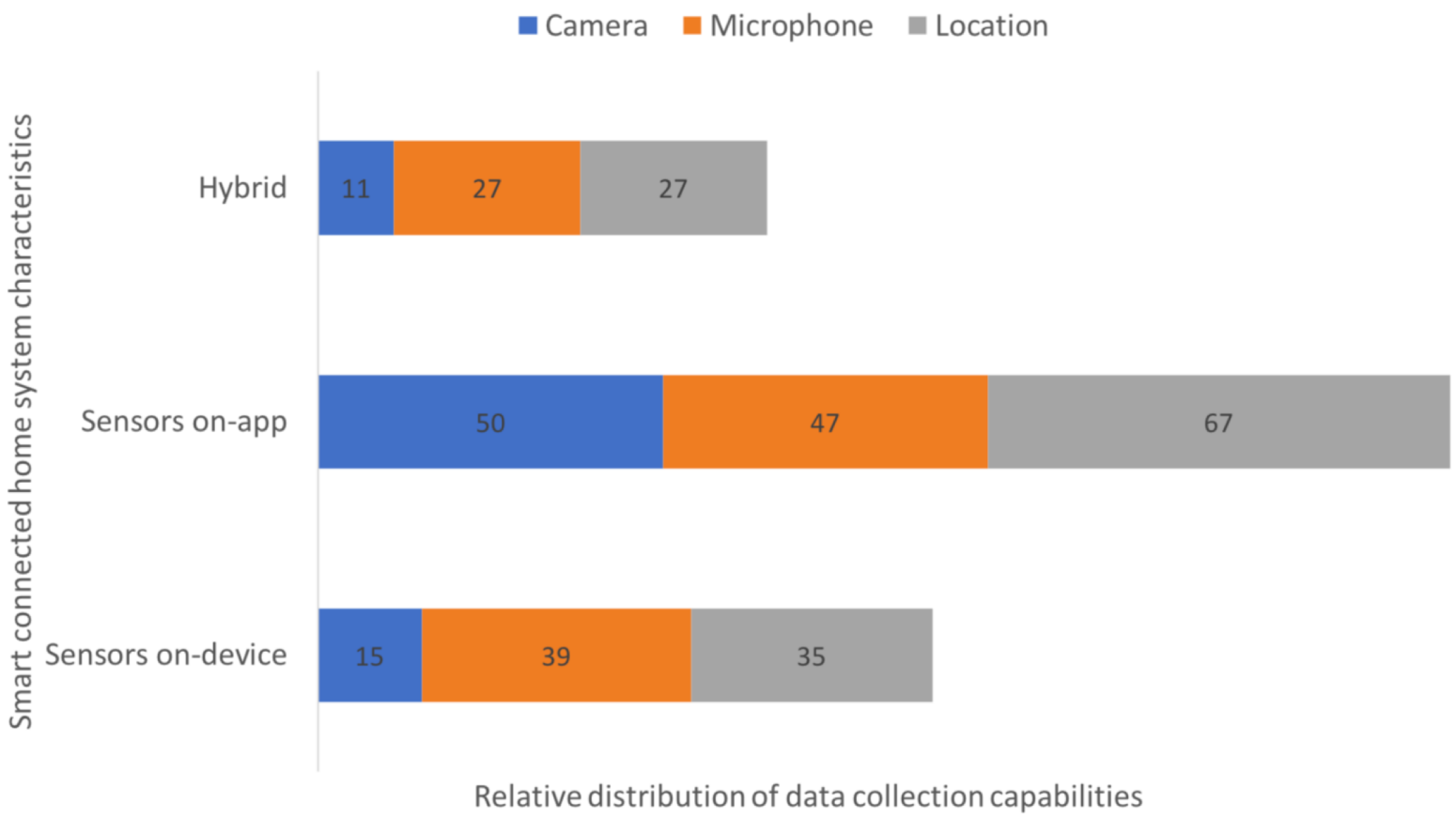
E.g., Fitbit Ionic Watch.

Watchers

Collect the behavior of users typically by using sensors embedded inside the connected device.

E.g., Nest Cam Indoor Security Camera.

ANALYSIS OF SYSTEMS



SOME BEST PRACTICES

- ✓ **Controlling data collection.** Data subjects should be provided the possibility to opt-in for data collection, and thus data will not be collected unless the user decides so, or otherwise have the option to opt-out of such data collection.

- ✓ **Transparency about data collection.** Data subjects should be made aware of details of data that are being collected about them, the purpose or benefit gained for such collection, the location of data collection, and whether that data are retained or shared with other parties.

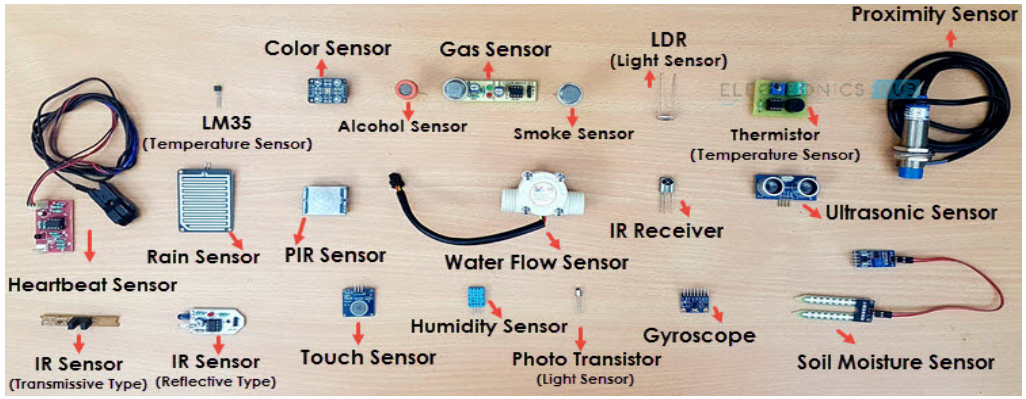
- ✓ **Ethical uses of collected data.** Manufacturers should indicate what inferences can be made with the collected data and likewise the sensors that are being used for making those inferences.

CONCLUSIONS

- ✓ The growth and heterogeneity of smart connected home systems raise the importance of a classification that groups systems into categories indicative of their data exposure.
- ✓ We developed a novel four-tiered classification of smart connected home systems clustering them into: app-based accessors, watchers, location harvesters, and listeners.
- ✓ The classification can also include general-purpose and multi-functional devices, and can be automatically recreated any point with updated data.
- ✓ Overall, the presented classification and analysis can help us better understand the privacy implications and what is at stake with different smart connected home systems.

FUTURE WORK

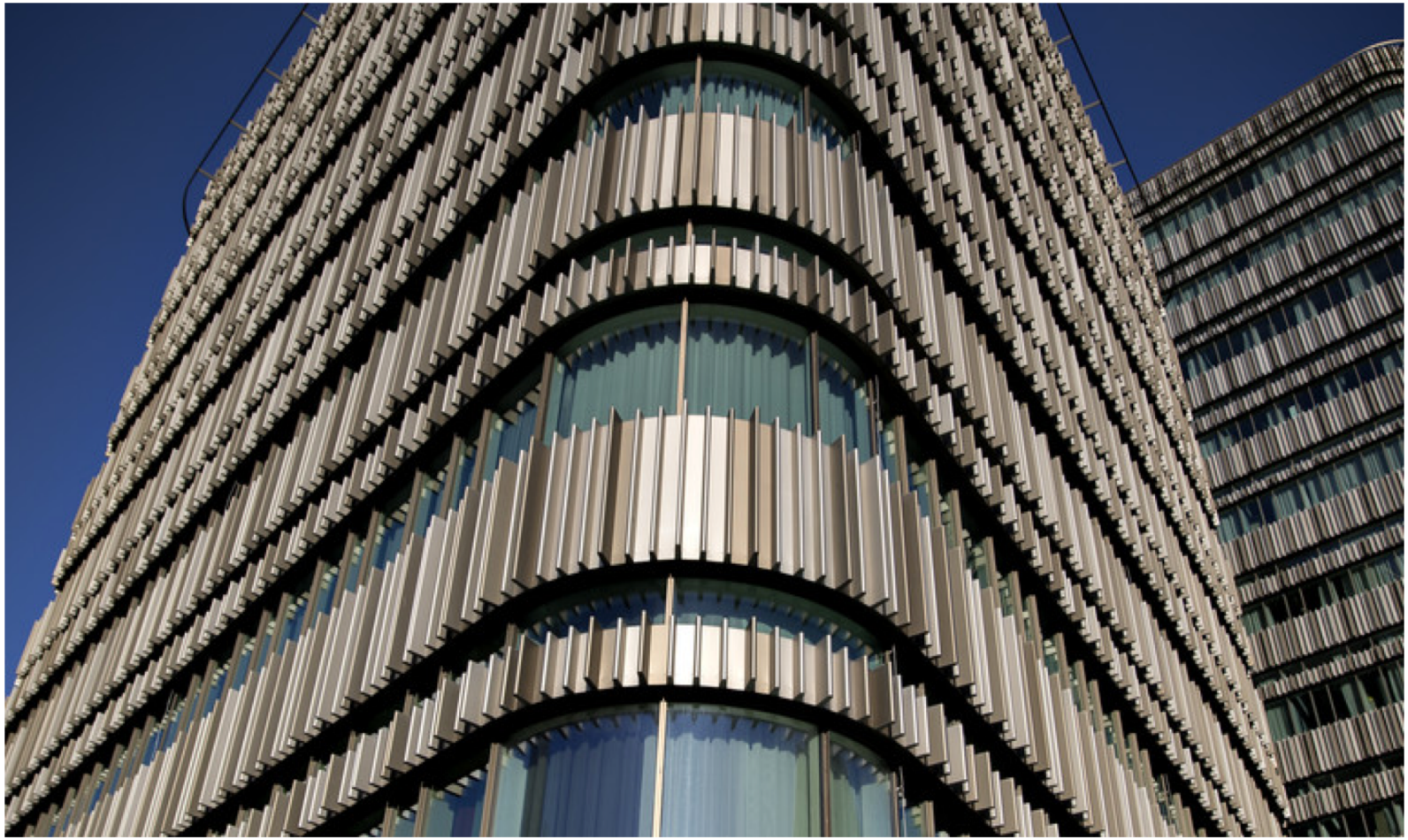
✓ Analyze a broader range of systems



✓ Explore other data types

✓ Use of quantitative metrics for privacy risk analysis

Thank you for your attention!



Source: mau.se

Joseph Bugeja
joseph.bugeja@mau.se

Andreas Jacobsson
andreas.jacobsson@mau.se

Paul Davidsson
paul.davidsson@mau.se